11-08-00   A

Please type a plus sign (+) inside this box → ☐

UTILITY
PATENT APPLICATION
TRANSMITTAL

(Only for new nonprovisional applications under 37 C.F.R. § 1.53(b))

Attorney Docket No.	1280.00272
First Inventor or Application Identifier	Paul W. Dent et al.
Title	Method for Masking Secret Multiplicands
Express Mail Label No.	EM414006772US

APPLICATION ELEMENTS

See MPEP chapter 600 concerning utility patent application contents.

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

1. [X] * Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original and a duplicate for fee processing)

2. [X] Specification [Total Pages 35]
(preferred arrangement set forth below)
- Descriptive title of the Invention
- Cross References to Related Applications
- Statement Regarding Fed sponsored R & D
- Reference to Microfiche Appendix
- Background of the Invention
- Brief Summary of the Invention
- Brief Description of the Drawings (if filed)
- Detailed Description
- Claim(s)
- Abstract of the Disclosure

3. [X] Drawing(s) (35 U.S.C. 113) [Total Sheets 2]

4. Oath or Declaration [Total Pages 2]
a. [X] Newly executed (original or copy)
b. [ ] Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 16 completed)
i. [ ] DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).

*NOTE FOR ITEMS 1 & 13: IN ORDER TO BE ENTITLED TO PAY SMALL ENTITY FEES, A SMALL ENTITY STATEMENT IS REQUIRED (37 C.F.R. § 1.27), EXCEPT IF ONE FILED IN A PRIOR APPLICATION IS RELIED UPON (37 C.F.R. § 1.28).

5. [ ] Microfiche Computer Program (Appendix)

6. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
a. [ ] Computer Readable Copy
b. [ ] Paper Copy (identical to computer copy)
c. [ ] Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

7. [ ] Assignment Papers (cover sheet & document(s))
8. [ ] 37 C.F.R.§3.73(b) Statement (when there is an assignee) [ ] Power of Attorney
9. [ ] English Translation Document (if applicable)
10. [ ] Information Disclosure Statement (IDS)/PTO-1449 [ ] Copies of IDS Citations
11. [ ] Preliminary Amendment
12. [X] Return Receipt Postcard (MPEP 503) (Should be specifically itemized)
13. [ ] * Small Entity Statement(s) (PTO/SB/09-12) [ ] Statement filed in prior application, Status still proper and desired
14. [ ] Certified Copy of Priority Document(s) (if foreign priority is claimed)
15. [ ] Other: _____

16. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

[ ] Continuation [ ] Divisional [ ] Continuation-in-part (CIP) of prior application No: _____/_____

Prior application information: Examiner _____ Group / Art Unit _____

For CONTINUATION or DIVISIONAL APPS only: The entire disclosure of the prior application, from which an oath or declaration is supplied under Box 4b, is considered a part of the disclosure of the accompanying continuation or divisional application and is hereby incorporated by reference. The incorporation can only be relied upon when a portion has been inadvertently omitted from the submitted application parts.

17. CORRESPONDENCE ADDRESS

[ ] Customer Number or Bar Code Label
(Insert Customer No. or Attach bar code label here)
or [X] Correspondence address below

Name	F. William McLaughlin
	Wood, Phillips, VanSanten, Clark & Mortimer
Address	500 West Madison Street, Suite 3800

City	Chicago	State	Illinois	Zip Code	60661-2511
Country	U.S.A.	Telephone	312.876-1800	Fax	312.876-2020

Name (Print/Type)	F. William McLaughlin	Registration No. (Attorney/Agent)	32,273
Signature		Date	Nov. 7, 2000

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

FEE TRANSMITTAL
for FY 2001

Patent fees are subject to annual revision

Complete if Known

Application Number	Unassigned
Filing Date	Herewith
First Named Inventor	Paul W. Dent et al.
Examiner Name	
Group Art Unit	
Attorney Docket No.	1280.00272

TOTAL AMOUNT OF PAYMENT ($) 1,250.00

METHOD OF PAYMENT

1. [X] The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number: **23-0785**

Deposit Account Name: **Wood, Phillips et al.**

[X] Charge Any Additional Fee Required Under 37 CFR 1.16 and 1.17

[ ] Applicant claims small entity status. See 37 CFR 1.27

2. [X] **Payment Enclosed:**
[X] Check [ ] Credit card [ ] Money Order [ ] Other

FEE CALCULATION

1. BASIC FILING FEE

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee ($)	Fee Code	Fee ($)		
101	710	201	355	Utility filing fee	$710
106	320	206	160	Design filing fee	
107	490	207	245	Plant filing fee	
108	710	208	355	Reissue filing fee	
114	150	214	75	Provisional filing fee	

SUBTOTAL (1) ($)710.00

2. EXTRA CLAIM FEES

	Extra Claims	Fee from below	Fee Paid
Total Claims	50 -20** = 30	x $18	= $540
Independent Claims	3 - 3** = 0	x	=
Multiple Dependent			=

Large Entity		Small Entity		Fee Description
Fee Code	Fee ($)	Fee Code	Fee ($)	
103	18	203	9	Claims in excess of 20
102	80	202	40	Independent claims in excess of 3
104	270	204	135	Multiple dependent claim, if not paid
109	80	209	40	** Reissue independent claims over original patent
110	18	210	9	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)540.00

**or number previously paid, if greater; For Reissues, see above

---

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity		Small Entity		Fee Description	Fee Paid
Fee Code	Fee ($)	Fee Code	Fee ($)		
105	130	205	65	Surcharge - late filing fee or oath	
127	50	227	25	Surcharge - late provisional filing fee or cover sheet	
139	130	139	130	Non-English specification	
147	2,520	147	2,520	For filing a request for ex parte reexamination	
112	920*	112	920*	Requesting publication of SIR prior to Examiner action	
113	1,840*	113	1,840*	Requesting publication of SIR after Examiner action	
115	110	215	55	Extension for reply within first month	
116	390	216	195	Extension for reply within second month	
117	890	217	445	Extension for reply within third month	
118	1,390	218	695	Extension for reply within fourth month	
128	1,890	228	945	Extension for reply within fifth month	
119	310	219	155	Notice of Appeal	
120	310	220	155	Filing a brief in support of an appeal	
121	270	221	135	Request for oral hearing	
138	1,510	138	1,510	Petition to institute a public use proceeding	
140	110	240	55	Petition to revive - unavoidable	
141	1,240	241	620	Petition to revive - unintentional	
142	1,240	242	620	Utility issue fee (or reissue)	
143	440	243	220	Design issue fee	
144	600	244	300	Plant issue fee	
122	130	122	130	Petitions to the Commissioner	
123	50	123	50	Petitions related to provisional applications	
126	240	126	240	Submission of Information Disclosure Stmt	
581	40	581	40	Recording each patent assignment per property (times number of properties)	
146	710	246	355	Filing a submission after final rejection (37 CFR § 1.129(a))	
149	710	249	355	For each additional invention to be examined (37 CFR § 1.129(b))	
179	710	279	355	Request for Continued Examination (RCE)	
169	900	169	900	Request for expedited examination of a design application	

Other fee (specify) _____

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) ($)

SUBMITTED BY			Complete (if applicable)	
Name (Print/Type)	F. William McLaughlin	Registration No. (Attorney/Agent) 32,273	Telephone	312.876-1800
Signature			Date	Nov. 7, 2000

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

APPLICATION FOR

UNITED STATES LETTERS PATENT

SPECIFICATION

TO ALL WHOM IT MAY CONCERN:

Be it known that **PAUL W. DENT**, a citizen of GREAT BRITAIN, residing at 637 Eagle

Point Road, Pittsboro, in the County of Chatham and State of NORTH CAROLINA, and

MICHAEL KORNBY, a citizen of SWEDEN, residing at 125 Lochwood West Drive, Cary, in the

County of Wake and State of NORTH CAROLINA, have invented a new and useful **METHOD**

FOR MASKING SECRET MULTIPLICANDS of which the following is a specification.

METHOD FOR MASKING SECRET MULTIPLICANDS

FIELD OF THE INVENTION

The invention relates to implementation of public/private key encryption in tamper-proof chips.

5   Certain wireless mobile communications systems, such as the global system for mobile communications (GSM) uses a removable subscriber identity module (SIM), also referred to as a "smart card". The SIM stores various subscriber related data, such as an IMSI value, which is referred to in the GSM system as an international mobile subscriber identity. The SIMs are conventionally pre-programmed to include the IMSI. Thus, a mobile communications system

10   operator typically purchases a supply of SIMs. The mobile terminals themselves do not include information that identifies the subscriber. Instead, the mobile station is a shell until the SIM is installed. The SIM can be removed from one mobile terminal and inserted in a new mobile terminal. This enables the new mobile terminal to be used immediately. This also renders the SIM open to attacks to the stored data. Therefore, security methods, such as public/private key encryption can

15   be used to secure the stored data.

Public/private key encryption methods are based on the identity

$$\left| X^Z \right|_N = X,$$

where the modulus N is the product of two secret primes P1, P2 and Z is equal to $M(P1-1)(P2-1)+1$ and M is arbitrary.

Z is factorized into the product of a private key Kpriv and a public key Kpub.

Many pairs of these can be found by choosing different values of M. Kpub is published and may

be used by another party to send messages, which can only be deciphered by the recipient using

Kpriv.

5   The known RSA algorithm enciphers blocks of bits at a time, which, viewed as a

binary number X, must have an arithmetic value less than the given modulus N. Encryption is

accomplished by raising X to the power Kpub, and reducing it modulo-N. Decryption does the

same using Kpriv to reproduce X. All such operations necessarily produce a result less than N.

Another use of the public/private key pair is for signing messages to prove they

10   were sent by a particular party. The party then encrypts the message using Kpriv and any party

can decipher it with Kpub, and will obtain a sensible result only if the message was encrypted

using the senders secret private key Kpriv.

When both encryption and signing are required, the message is signed using the

sender's private key Kpriv1 and modulus N1 and then ciphered using the recipient's public key

15   Kpub2 and modulus N2. The recipient replies in the same way using Kpriv2 and Kpub1, and the

moduli NI and N2 reversed.

In both cases, during either signing a message to be transmitted or deciphering a

message received, a computational circuit is required to raise a large binary number to the power

of Kpriv without releasing or betraying Kpriv to the world outside a secure, tamper-proof circuit.

20   Reference is made to Bruce Schneier's book "Applied Cryptography" (John Wiley

and Sons, 1994) for further understanding of the prior art. This book is hereby incorporated by reference herein in its entirety.

Two main algorithms are known for reducing the effort in raising a number as large as 2048 bits to a power that can be a number almost as long in bits, and reducing it modulo

5   another large number.

If the power Kpriv is a bitstring B_n, B_{n-1}.....B_3, $B_{2,1}$ B_1, then X raised to this power is given by

$$Z = 1 \quad \text{times X (if Bl=1)}$$

$$\text{times } X^2 \text{ (if B2 = 1)}$$

10                   $$\text{times } X^4 \text{ (if B3 = 1)}$$

$$\cdots$$

$$\cdots$$

and so forth.

Thus successive squares x, x^2, $(x^2)^2$ .... are formed, and either multiply the Z-

15   accumulator or not depending if a corresponding bit is 1 or 0. Thus the number of numbers that have to be multiplied to form Z is only of the order of 2048 instead of 2^{2048}, which would be impractical. This successive squaring algorithm is vital in rendering such calculations tractable.

After each multiplication or squaring, which increases-the original word length from 2048 to 4096 bits, the word length is decreased back to 2048 bits by reducing the result

20   modulo-N. This requires subtracting a number of multiples of N until the result is less than N.

The number of multiples of N which have to be subtracted is of the order of two to the power 2048 or 10^{600} which clearly eliminates the possibility of successive subtraction. Instead, since the modulus (N) is fixed for a long time, its approximate reciprocal may be computed to 2048 significant bits, ignoring leading zeros after the binary point, and stored as 1/N (approximately).

5   Then each time a 4096-bit Z value is to be reduced modulo-N, the approximate number of times N would have to be subtracted is calculated from $T = Z \times (1/N)$ which is just a single long multiplication of Z with the stored approximate reciprocal. T times N is then subtracted from Z which will be found to have reduced it to within one or two times N of the required result. The reduction is completed by subtracting N one or two times more from Z until the remainder is less than N but not negative. This modulo-reduction algorithm thus requires about two long

10   multiplications and two subtractions instead of 10^{600} successive subtractions, and is also vital to render such calculations possible.

Other computation reduction algorithms take advantage of the fact that a squaring operation can be performed faster than a multiplication of two different quantities, as the same

15   partial products occur twice and need only be calculated once.

The pattern of calculation when employing these algorithms in a common fashion is thus:

1. Load X into the Z accumulator (Assuming Kpriv is odd so B1 = 1, else set Z =1)

2. Square X and reduce modulo-N

3. If B2 = 1, multiply the new value of X into the Z accumulator and reduce Z modulo-N

4. Repeat from step 2 using successively B3, B4, B5 etc. at step 3 until done.

5

In the above, the duration of one iteration of the loop depends on whether or not the conditional multiplication was performed at step 3. Therefore by observing whether the iteration was a short one or a long one by measuring power consumption profiles external to the circuit, it can be determined whether each value B2, B3, B4 was a one or a zero and therefore

10 determine the secret value Kpriv. In the prior art of cipher systems, such inadvertent leakage of secret information was termed a "TEMPEST" hazard after the acronym for the Government testing standards against which cipher equipment was tested. The problem was solved in the prior art of cipher systems by inclusion of special "RED" power supplies that maintained the same power consumption irrespective of the circuit activity, for example by the use of a shunt regulator.

15 However, in this prior art the RED power supplies were separate and not an integrated part of the cipher chips, as it was assumed that the threat did not have physical access to internal nodes of the equipment. However, if the cryptographic circuits are located on a removable card such as a SIM that is inserted into mobile terminals, then it is assumed that an ill-intentioned person might sometime gain access to the SIM connections.

20 There is thus a need for a circuit and method which can raise large numbers to a

large power without inadvertently betraying the power through a TEMPEST leak.

PCT publication number WO 99/63696 describes the incorporation of a random number generator or noise source to randomize the timing of calculations so that power profile is not so obviously correlated with secret information. The above PCT application is hereby

5   incorporated by reference herein. This technique is not completely effective however, as multiple observations can be made to determine the shortest delay between different power profile patterns, which presumably correspond to the addition of zero or small random delay. Therefore there is a need for improved methods to conceal the nature of internal calculations with secret information.

SUMMARY OF THE INVENTION

10   The above needs are met in a computational device for performing secret cryptographic calculations with secret numbers, using a method of hiding secret information from outside observation by scheduling the calculations using a precomputed, fixed randomization of the schedule in such a way that externally observable parameters of the device cannot be associated to particular pieces, bits, symbols or values of the secret information.

15   BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a generalized block diagram illustrating a mobile terminal having a SIM implementing cryptographic calculations in accordance with the method of the present invention; and

Fig. 2 is a block diagram of the SIM of Fig. 1.

DETAILED DESCRIPTION OF THE INVENTION

Referring to Fig. 1, a mobile terminal 10 is illustrated in block diagram form. In the illustrated embodiment of the invention, the mobile terminal 10 comprises a GPRS-136HS mobile terminal. This type of mobile terminal 10 is used in a time-division multiple access (TDMA) mobile

5   communications system network. The mobile terminal 10 includes a subscriber identity module (SIM) 12 also known as a SIM card or smart card. The SIM card 12 is generally similar to SIM cards used in global system for mobile communications (GSM) systems which contains unique subscriber information. In accordance with the invention, a method is disclosed for masking secret multiplicands used for public/private key encryption for the mobile terminal 10 including the SIM card

10   12. While the method is described in connection with a mobile terminal used in a TDMA system, the inventive method could be used in other types of mobile communications systems, including a code-division multiple access (CDMA) system, such as IS95 or Universal Mobile Telephone System (UMTS).

The mobile terminal 10 includes an antenna 14 for sending and receiving through-the-air radio

15   signals between itself and a mobile communications system network. The antenna 14 is connected to a transmitter/receiver 16 to broadcast and receive on the same antenna 14. Particularly, the transmitter/receiver 16 includes a receiver that demodulates, de-multiplexes, and decodes the radio signals into one or more channels. Such channels include a control channel and a traffic channel for speech or data. The speech or data are delivered to an output device of an input-output circuit 18,

20   such as a speaker. The receiver delivers messages from the control channel to a processor 20. The

processor 20 controls and coordinates the functioning of the mobile terminal 10 responsive to

messages on the control channel using programs and data stored in a memory 22 and the SIM card

12 so that the mobile terminal 10 can operate within the mobile communications system network.

The processor 20 also controls the operation of the mobile station 10 responsive to input from the

5   input-output circuit 18. This input may utilize a keypad or the like as a user-input device and a

display to give the user information, as is well known. The transmitter/receiver 16 also includes a

transmitter that converts analog electrical signals into digital data, encodes the data with error-

detection and correction information, and multiplexes this data with control messages from the

processor 20. This combined data is modulated and broadcast via radio signal through the antenna

10   14, as is conventional. The memory 22, in accordance with the invention, stores information relating

to the capabilities of the mobile terminal 10 as well as information personalized to the particular

mobile communications system network operator.

The present invention is described herein in the context of a mobile terminal. As used

herein, the term "mobile terminal" may include a mobile communications radiotelephone with or

15   without a multi-line display; a Personal Communications System (PCS) terminal that may combine

a mobile communications radiotelephone with data processing, facsimile and data communications

capabilities; a PDA that can include a radiotelephone, pager, Internet/intranet access, Web browser,

organizer, calendar and/or a global positioning system (GPS) receiver; and a conventional laptop

and/or palmtop receiver or other appliance that includes a radiotelephone transceiver. Mobile

20   terminals may also be referred to as "pervasive computing" devices.

-8-

The SIM card 12 stores subscriber related data. In accordance with the invention, the

SIM card 12 is configured as a tamper-proof device for performing discrete exponentiations,

modulo a very large number. Referring to Fig. 2, the SIM card 12 comprises a control processor

24, a multiplier 26 for accelerating cryptographic calculations, and memory 28, and is covered

5   by an upper metallization layer (not shown) to prevent probing internal nodes for the illicit

purpose of extracting stored secret information, and in particular a private key that is often used

as an exponent. The processor 24 is connected to an input/output interface connector 30 for

operative connection to the mobile terminal processor 20, see Fig. 1. The connector 30 enables

subscriber data to be stored on the SIM card 12 and for data to be transferred between the

10   processors 24 and 20. When the private key is used as the exponent to exponentiate a large

number, the large number is successively squared and the result either multiplies an accumulator,

if the corresponding bit of the private key equals 1, or not if the bit is 0. In the prior art,

observation of the power supply current profile external to the tamper-proof chip could betray

whether a multiplication with the accumulator took place or not and thereby reveal the bits of the

15   private/secret key. The chip therefore also preferably comprises a shunt regulator 32 to ensure,

as far as possible, that the current consumption of the chip in the middle of a calculation period

is held approximately constant and independent of the values calculated. Nevertheless, small

externally observable changes such as magnetic fields may still betray internal activity.

Particularly, the SIM card 12 comprises a tamper-proof computational device. The

20   connector 30 comprises an input/output interface. The memory 28 stores secret information in

the form of, for example, the subscriber related data. The processor 24 is programmed for performing secret cryptographic calculations. These calculations use secret numbers, such as the private key and hide the stored secret information from outside observation by scheduling the cryptographic calculations using a precomputed, fixed randomization schedule in such a way that

5   externally observable parameters cannot be associated to particular pieces, bits, symbols or values of the secret information.

In one implementation, the invention comprises the processor 24 and the cryptographic multiplier 26 performing a small number of false multiplications, the results of which are sent to a "waste basket" or at least do not replace the old accumulator value, when a

10   multiplication with the accumulator would ordinarily not have been performed. For example, if the key is a 1500 bit number having typically 750 1's and 750 0's, inserting 25 false multiplications at random where there is a zero only increases execution time by 3%. However, attempting to extract the private key then involves determining which 25 out of 750 multiplications were false, which requires $^{750}C_{25}$ trials, an impossibly big number.

15   In another implementation, successive squares with modulo-reduction are performed a small number of times, for example eight, and the results stored in eight memory locations. Then the first byte of the private key is used to determine which of the eight values to multiply with the accumulator, according to whether a 1 is in the corresponding bit position of the byte. As each value is multiplied, the corresponding bit in the byte is set to zero, and a new successive

20   square is then computed and overwrites the square just used in the eight memories. If the bit is

zero and a square is not used, a successive square is performed anyway and overwrites the square

not used. When the bits of the byte have all been tested, the next most significant byte of the

private key is fetched and the process continues. By so interlacing the computation of successive

squares, whether or not they are used to multiply the accumulator, it is difficult to determine

5   which of the precomputed terms were used in multiplication.

In a third implementation, at the time the private key Kpriv is generated it is

partitioned into three values K1, K2, K3 such that $K1 \cdot K2 + K3 = Kpriv$, each being of half the

word length of Kpriv, and furthermore such that the total number of 1's in K1, K2 and K3 together

is minimized and smaller than the total number of 1's in Kpriv. When a value is to be

10   exponentiated with Kpriv, successive squares are formed as before and multiplied to two

accumulators according to the bits of K1 and K3 respectively thus forming the value raised to the

power K1 as Z1 and the value raised to the power K3 as Z3. The value Z1 is then further raised

to the power K2 by successively squaring Z1 and accumulatively multiplying the successive

squares (or not) dependent on if a bit of K2 is a 1, or 0, to obtain Z2. Finally, the product of Z2

15   and Z3 is formed and modulo-reduced to produce the desired result.

Any combination of the above three methods may also be used to eliminate the

correlation between power profile and secret information usage.

The essential algorithms for performing public key cryptographic calculations and

their deficiencies were described above. To mask internal activity in cipher circuits, it was

20   already known in the prior art to employ special "RED" power supplies to keep externally

-11-

observable current consumption fluctuations to a minimum. Such a power supply can comprise a constant current source to draw a constant current from the supply, followed by a shunt voltage regulator which bypasses current to ground that is not instantaneously consumed. It may be difficult to fully integrate an effective RED supply on to a tamper-proof chip, such as on a SIM card, however, because the current source needs to supply the peak current drain on a continuous basis; unless averaged by a substantial capacitor. However, the peak current drawn by high speed logic circuits can be very large. There is a limit to how well such analog components as current sources, shunt regulators and smoothing capacitors can be integrated with a logic circuit, and so this invention discloses other means and methods to mask internal activity of logic circuits. The invention also seeks to mask deducing secret information by observing any other externally observable parameter of the circuit, such as the timing of output signals from the device.

In order to mask the bits of the secret key, a first implementation of the invention comprises modifying the sequence of calculations implemented in the SIM card processor 24 to mask the secret multiplicands by inserting a small percentage of additional multiplications as follows:

1.   Load X (or 1) into the Z accumulator according as $B1=1$ or 0, and into a dummy accumulator Z'

2.   Square X and reduce modulo-N

3.   (a)   If $B2 = 1$, multiply the new value of X into the Z accumulator and reduce Z modulo-N, else

(b)   If B2 = 0 but a randomizing indicator is set, multiply the new value

of X with Z (or Z') and reduce modulo-N, but store the result in the dummy location Z'

4.   Repeat from step 2 using successively B3,B4,B5 etc at step 2 until done.

When the randomizing indicator is set, a loop iteration that would otherwise have

5   been short, due to a bit of Kpriv being zero, is lengthened to the same length as if Kpriv had been

1. A loop iteration for which the corresponding bit of Kpriv equals 1, is however always long.

Therefore, if the randomizing indicator were different on different occasions when Kpriv was

used, as in PCT patent WO 99/63696, observing those loop iterations that were always long and

those loops that were sometimes short on different occasions would still betray the value of Kpriv.

10   Therefore according to this invention, the randomizing indicator bits must always be the same and

preferably determined once and for all at the time Kpriv is generated. The randomizing indicator

is therefore a binary word of the same length as Kpriv, having a binary one, in about one in thirty

of the positions where Kpriv has a zero. It is of no consequence if the randomizing word also has

1's where Kpriv has 1's, so the randomizing word of perhaps 2048 bits must just contain about

15   2048/30, or about 64, binary 1's. The randomizing word can be generated at the time Kpriv is

generated by generating a random number between 0 and 2047 to determine the bit address of the

randomizing word that shall be set to 1, and repeating this 64 times to place about 64 1's in the

word. The randomizing word can then be permanently stored along with Kpriv, and is designated

by Krand.

20   When the above methods are used, it may still be possible to determine which

-13-

iterations are long and which are short, but the value of Kpriv so betrayed is modified to Kpriv.OR.Krand which has extra 1's in about 32 bit positions where Kpriv had zeroes. It is however impossible to distinguish which 1's are real and which are false. It is not a question of just trying 2^{32} possibilities, but, assuming there are in total about 750 1's in the composite value

5   Kpriv.OR.Krand, of testing which 32 out of 750 should really be zeros. Moreover, whether the number of false 1's is exactly 32 is not known for sure, the uncertainty being perhaps between 20 and 60. While the position of nearly all the zeros in Krand may be observed, there is a very large uncertainty remaining in the value of Kpriv.

The second implementation of masking the secret multiplicand by breaking the

10   correlation between power supply current fluctuations and internal computational activity is now disclosed. Since all successive squares of X are computed, it is theoretically possible to compute them all first and store the results in 2048, 2048-bit memories that is in a 4 megabit memory. Then the bits of Kpriv which are 1 are used to select from the memory those 2048-bit values which are to be multiplied. With the reasonable assumption that it is impossible to distinguish

15   selection of one value to multiply the accumulator from another, only the total number of values selected, that is the total number of 1's contained in Kpriv is betrayed, but not their bit positions. To mask the slight difference in current profile timing that might occur as a 0 in Kpriv is skipped, testing the next bit of Kpriv could advantageously be buried in the middle of an ongoing multiplication sequence. For example, if separate multiplication acceleration hardware is

20   employed, the control processor could locate the next 1 in Kpriv and prepare the corresponding

-14-

address within the 4 megabit memory for the next multiplication in parallel with performing the previous multiplication.

At the present time, a 4 megabit RAM requirement is expensive for the above method, but the method can be applied partially to subgroups of bits of Kpriv as follows:

1. Since Kpriv is almost always odd, multiplication with X is always required and can be initially loaded into the Z-accumulator;

2. Compute 8 successive squares of X and store in 8, 2048-bit locations, numbered 0 to 7, a RAM usage of 2048 bytes;

3. Locate the next most significant 1, in the first byte of Kpriv and multiply Z by the value in the corresponding one of the 8 memories, if the value is available; otherwise continue to step 4;

4. Compute a new successive square of X and store in memory location $|n+1|_8$,

5. Repeat from step 3 using bits from successive bytes of Kpriv until done.

An example of the above calculation sequence is given for the case where Kpriv comprises the bit pattern 111001010010101101011001

Designating squaring of X by "SQ" and storing of the result in a memory location 'j' by SQ -> j, and designating multiplication of the Z-accumulator with the value from storage location 'i' by MPY(i), the following sequence is obtained:

SQ -> 0

SQ -> 1
SQ -> 2
SQ -> 3
SQ -> 4
5   SQ -> 5
SQ -> 6
SQ -> 7
MPY(2)   (corresponding to the '1' of Kpriv 4th bit from the right)
SQ -> 0   (that square was not needed so can be overwritten)
10   MPY(3)
SQ -> 1   "
MPY(4)
SQ -> 2
MPY(6)
15   SQ -> 3
MPY(0)   (The '1' in the LSB position of the second byte of Kpriv)
SQ -> 4
MPY(1)
SQ -> 5
20   MPY(3)
SQ -> 6
MPY(5)
SQ -> 7
SQ -> 0   (The next '1' in Kpriv is bit 0 of the third byte and that square was
25   not yet calculated)
MPY (0)
SQ -> 1
SQ -> 2   (The next '1' in Kpriv is bit 2 and that square was not
                    yet calculated)
30   MPY(2)
SQ -> 3
SQ -> 4
SQ -> 5
MPY(5)
35   SQ -> 6
MPY(6)
SQ -> 7
MPY(7)

Assuming that a squaring operation can be detected externally to the circuit to differ

from a multiplication operation, it can be detected from the above sequence that eight consecutive

multiply/square steps were interrupted a double square step before the next multiply. This betrays

the fact that a new value in memory number 0 was needed but was not yet available. Therefore

it is detectable that the LSB of the third byte of Kpriv is a 1. It is also evident that the first two

5   bytes of Kpriv contained eight 1's, but their locations are concealed. Unfortunately the next double

square also reveals that bit 2 of the third byte of Kpriv is a 1, and the following triple square

reveals that bit 5 is a 1, and so forth. To obtain the same level of concealment as for the first 16

bits of Kpriv, the sequence should be modified as follows:

```
          SQ -> 0
10        SQ ->  1
          SQ ->  2
          SQ ->  3
          SQ ->  4
          SQ ->  5
15        SQ ->  6
          SQ ->  7
          MPY(2)      (corresponding to the '1' of Kpriv 4th bit from the right)
          SQ -> 0     (that square was not needed so can be overwritten)
          MPY(3)
20        SQ -> 1
          MPY(4)
          SQ -> 2
          MPY(6)
          SQ -> 3
25        MPY(0)      (The '1' in the LSB position of the second byte of Kpriv)
          SQ -> 4
          MPY(1)
          SQ -> 5
          MPY(3)
30        SQ -> 6
          MPY(5)      At this point the next square needed is not yet
```

calculated; that means that all of the values in the
8 memories are done with and may be overwritten; so
8 new successive squares are calculated

SQ ->7

5   SQ -> 0

SQ -> 1

SQ -> 2

SQ -> 3

SQ -> 4

10   SQ -> 5

SQ -> 6

MPY (0)

SQ -> 7

MPY (2)

15   SQ -> 0

MPY (5)

SQ -> 1

MPY (6)

SQ -> 2

20   MPY (7)

SQ -> 3   At this point let us assume that the next square needed
is some way ahead and not yet calculated. Thus all
memorized squares are done with and a new 8 may be
calculated.

25   SQ -> 4

SQ -> 5

SQ -> 6

SQ -> 7

SQ -> 0

30   SQ -> 1

SQ -> 2

From the above sequence it may be deduced that, after the MPY(5) instruction an

MPY(6) instruction was not the next needed multiplication, and therefore that the corresponding bit

of Kpriv was a zero. However, the positions of the implied 1's in Kpriv corresponding to the next

five MPY instructions:

MPY(O), MPY(2), MPY(5), MPY(6), MPY(7) are concealed, as the sequence could

equally well have comprised

MPY(1), MPY(2), MPY(3), MPY(5), MPY(7) or

5   MPY(O), MPY(l), MPY(4), MPY(5), MPY(6) or any such combination.

Thus after processing 256 bytes of Kpriv, the numerical uncertainty in its value still

remaining is enormous.

The first method of concealment by insertion of a small number of false multiplications

can also obviously be combined with the above second method. A variation on the insertion of false

10   multiplications can also be used, which is to convert one of each pair of immediately successive

squaring operations from the "efficient" squaring method to the normal long multiplication method

applicable to unequal multiplicands, so that a double square operation SQ SQ is not distinguishable

from MPY SQ or SQ MPY. Whether the first or the second SQ is so-converted can be random, but

predetermined, and the center SQ operation of three in succession would always be converted to a

15   MPY look-alike.

Since the bits of Kpriv are long-term fixed, the above sequences may be predetermined

and stored as a preferred instruction sequence that best conceals Kpriv. Since it is desirable that Kpriv

never be revealed outside the tamper-proof area, the program to compute these sequences should be

stored on the same chip.

20   In a third implementation, a method of exponentiating by Kpriv is sought which not

only helps to conceal its value, but also reduces the effort needed to perform the exponentiation.

It can be advantageous to search for factors of Kpriv first and remove them, as it takes little effort to apply exponentiation by small prime factors at the end. The problem then reduces to one of exponentiating by the remaining value of Kpriv after removing at least small prime factors that

5 can be discovered quickly. The remaining value of Kpriv after removing all the discovered factors, including 2, will of course be odd.

An exemplary 2048-bit odd value Kpriv may be partitioned into three 1024-bit values K1,K2 and K3 such that K1 · K2+K3 = Kpriv

in innumerably different ways, some of which will result in K1, K2 and K3 containing fewer 1's than

10 others.

By choosing a partitioning having a minimum total number of 1's, the effort needed to exponentiate by Kpriv can be reduced with regard to the equation

$$X^{kpriv} = (X^{K1})^{K2} \cdot X^{K3}$$

Each of the exponentiations by K1, K3 and K2 requires an effort related to the number

15 of 1's contained in the power and thus the total effort may be reduced if the total number of 1's in K1,K2 and K3 together is less than the number of 1's in Kpriv.

Other partitioning such as

$$K1 \cdot K2+K3 \cdot K4 = Kpriv$$

could also be used.

20 Another partitioning option comprises expressing Kpriv as the product of sparse

integers $K1 \cdot K2 \cdot K3$ .... plus a remainder R, where K_i is of the form 2^i+1, and then exponentiating X

first by the largest factor and by R simultaneously to form Z1 and Z2, and then successively

exponentiating Z1 further by the smaller K-factors, multiplying the final Z1 value by Z2,

i.e. computing $X^R \times (((((X^{Kn})^{Kn-1})..)..)^{K2})^{K1}$.

5   The effort required for the latter is related to the number of binary ones in R plus the sum of the

binary ones in all the K-factors.

At the time Kpriv is generated, a program can be executed one time only to test

various partitions of the above form and to determine a partitioning most efficient for exponentiating

by Kpriv. The exact partitioning chosen will not however be known to the outside, so together with

10   the other safeguards disclosed above, the value with which exponentiation is being performed can be

hidden from external observers. A person skilled in the art may use the above teachings to implement

many variations for hiding the nature of internal calculations or accelerating exponentiation by a very

large power, or both, which nevertheless would fall within the scope and spirit of the invention if

adhering to the steps described in the attached claims.

15   The present invention has been described with respect to a block diagram of

programmed devices. It will be understood that the functions described relative to each block of the

block diagram can be implemented by computer program instructions. These program instructions

may be provided to a processor to produce a machine, such that the instructions, which execute on

the processor, create means for implementing the functions described relative to the blocks. The

20   computer program instructions may be executed by a processor to cause a series of operational steps

to be performed by the processor to produce a computer implemented method such that the

instructions which execute on the processor provide steps for implementing the functions specified

in the blocks. Accordingly, the illustrations and accompanying disclosure support combinations of

means for performing a specified function and combinations of steps for performing the specified

5   functions. It will also be understood that each block and combination of blocks can be implemented

by special purpose hardware-based systems that perform the specified functions or steps, or

combinations of special purpose hardware and computer instructions.

CLAIMS

We claim:

1.   In a computational device for performing secret cryptographic

2   calculations with secret numbers, a method of hiding secret information from outside observation

comprising:

4   scheduling said calculations using a precomputed, fixed randomization schedule in

such a way that externally observable parameters of the device cannot be associated to particular

6   pieces, bits, symbols or values of said secret information.

2.   The method of claim 1 in which scheduling said calculations comprises

2   inserting dummy calculations according to a schedule associated with one of said secret numbers

in the middle of calculations using the associated secret number.

3.   The method of claim 2 in which the schedule uses a randomizing indicator

2   in the form of a binary word having a length equal to that of the secret number and having a

binary one in a select number of places that the secret number has a binary zero.

4.   The method of claim 2 in which said dummy calculations affect a pattern

2   of variation of power supply current consumed by the device so as to mask any correlation

between power supply current variation and said secret information.

5. The method of claim 1 in which in which said externally observable

2 parameters include variation in power supply current.

6. The method of claim 1 in which said externally observable parameters

2 include variation in timing of outputting results of said calculations.

7. The method of claim 1 in which said secret cryptographic calculations

2 comprise exponentiating a long integer to the power of a large secret exponent.

8. The method of claim 7 in which exponentiating a long integer to the power

2 of a large secret exponent comprises forming successive squares of said long integer reduced

modulo a given modulus.

9. The method of claim 8 in which successive squares are performed in groups

2 of a fixed length and the results temporarily stored.

10. The method of claim 9 further comprising selecting to multiplicatively

2 accumulate certain ones of said stored results dependent on if corresponding bits of one of said

secret exponents is binary one or binary zero in such a way that the stored results which are

4   selected cannot be determined from outside said device.

         11.   The method of claim 1 further comprising scheduling said calculations in

2   such a way as to reduce computational effort.

         12.   The method of claim 11 in which said calculations include exponentiating

2   a long integer to the power of a large secret exponent.

         13.   The method of claim 12 in which said large secret exponent is generated

2   upon first commissioning said device into operation and is internally stored and never released

outside the device.

         14.   The method of claim 12 in which said secret exponent is factorized into a

2   product of sparse integers plus a remainder such that the total number of ones in a binary

representation of said sparse integers and said remainder is a minimum.

         15.   The method of claim 13 further comprising generating in association with

2   said secret exponent and storing in association therewith a precomputed pseudorandom schedule

of dummy calculations to be inserted amidst calculations using said secret exponent.

16.   The method of claim 15 in which said schedule of dummy calculations

2   comprises dummy multiplications associated with a small fraction of the bits of said exponent

which are equal to one particular binary bit polarity.

17. A tamper-proof computational device comprising:

2 an input/output interface;

a memory storing secret information; and

4 a processor operatively connected to the input/output interface and to the memory,

the processor being programmed for performing secret cryptographic calculations with secret

6 numbers and hiding said stored secret information from outside observation by scheduling said

calculations using a precomputed, fixed randomization schedule in such a way that externally

8 observable parameters cannot be associated to particular pieces, bits, symbols or values of said

secret information.

18. The device of claim 17 wherein said processor schedules said calculations

2 by inserting dummy calculations according to the precomputed, fixed randomization schedule

associated with one of said secret numbers in the middle of calculations using the associated secret

4 number.

19. The device of claim 18 in which the processor uses a randomizing indicator

2 in the form of a binary word having a length equal to that of the secret number and having a

binary one in a select number of places that the secret number has a binary zero..

20.   The device of claim 18 in which said dummy calculations affect a pattern

2   of variation of power supply current consumed by the device so as to mask any correlation

between power supply current variation and said secret information.

21.   The device of claim 17 in which in which said externally observable

2   parameters include variation in power supply current.

22.   The device of claim 17 in which said externally observable parameters

2   include variation in timing of outputting results of said calculations.

23.   The device of claim 17 in which said secret cryptographic calculations

2   comprise exponentiating a long integer to the power of a large secret exponent.

24.   The device of claim 23 in which exponentiating a long integer to the power

2   of a large secret exponent comprises forming successive squares of said long integer reduced

modulo a given modulus.

25.   The device of claim 24 in which successive squares are performed in groups

2   of a fixed length and the results temporarily stored.

26.   The device of claim 25 wherein said processor selects to multiplicatively

2   accumulate certain ones of said stored results dependent on if corresponding bits of one of said

secret exponents is binary one or binary zero in such a way that the stored results which are

4   selected cannot be determined from outside said device.

27.   The device of claim 17 wherein said processor schedules said calculations

2   in such a way as to reduce computational effort.

28.   The device of claim 27 wherein said calculations include exponentiating

2   a long integer to the power of a large secret exponent.

29.   The device of claim 28 wherein said large secret exponent is generated upon

2   first commissioning said device into operation and is internally stored and never released outside

the device.

30.   The device of claim 28 wherein said secret exponent is factorized into a

2   product of sparse integers plus a remainder such that the total number of ones in a binary

representation of said sparse integers and said remainder is a minimum.

31.   The device of claim 29 wherein said processor generates in association with

2   said secret exponent and storing in said memory in association therewith a precomputed

pseudorandom schedule of dummy calculations to be inserted amidst calculations using said secret

4   exponent.

32.   The device of claim 31 wherein said schedule of dummy calculations

2   comprises dummy multiplications associated with a small fraction of the bits of said exponent

which are equal to one particular binary bit polarity.

33.   The device of claim 17 wherein device comprises a smart card.

34.   A mobile terminal used in a mobile communications system comprising:

2   a transmitter and a receiver for communicating in the mobile communications
system;

4   a controller controlling operation of the transmitter and the receiver; and

a tamper-proof device removably, operatively connectable to the processor and

6   comprising an input/output interface, a memory storing secret information, and a processor

operatively connected to the input/output interface and to the memory, the processor being

8   programmed for performing secret cryptographic calculations with secret numbers and hiding said

stored secret information from outside observation by scheduling said calculations using a

10   precomputed, fixed randomization schedule in such a way that externally observable parameters

cannot be associated to particular pieces, bits, symbols or values of said secret information.

35.   The mobile terminal of claim 34 wherein said processor schedules said

2   calculations by inserting dummy calculations according to the precomputed, fixed randomization

schedule associated with one of said secret numbers in the middle of calculations using the

4   associated secret number.

36.   The mobile terminal of claim 35 in which the processor uses a randomizing

2   indicator in the form of a binary word having a length equal to that of the secret number and

having a binary one in a select number of places that the secret number has a binary zero.

37.   The mobile terminal of claim 35 in which said dummy calculations affect

2   a pattern of variation of power supply current consumed by the device so as to mask any

correlation between power supply current variation and said secret information.

38.   The mobile terminal of claim 34 in which said secret cryptographic

2   calculations comprise exponentiating a long integer to the power of a large secret exponent.

39.   The mobile terminal of claim 38 in which exponentiating a long integer to

2   the power of a large secret exponent comprises forming successive squares of said long integer

reduced modulo a given modulus.

40.   The mobile terminal of claim 39 in which successive squares are performed

2   in groups of a fixed length and the results temporarily stored.

41.   The mobile terminal of claim 40 wherein said processor selects to

2   multiplicatively accumulate certain ones of said stored results dependent on if corresponding bits

of one of said secret exponents is binary one or binary zero in such a way that the stored results

4   which are selected cannot be determined from outside said device.

42.   The mobile terminal of claim 34 wherein said processor schedules said

2   calculations in such a way as to reduce computational effort.

43.   The mobile terminal of claim 42 wherein said calculations include

2   exponentiating a long integer to the power of a large secret exponent.

44.   The mobile terminal of claim 43 wherein said large secret exponent is

2   generated upon first commissioning said device into operation and is internally stored and never

released outside the device.

45.   The mobile terminal of claim 43 wherein said secret exponent is factorized

2   into a product of sparse integers plus a remainder such that the total number of ones in a binary

representation of said sparse integers and said remainder is a minimum.

46.   The mobile terminal of claim 44 wherein said processor generates in

2   association with said secret exponent and storing in said memory in association therewith a

precomputed pseudorandom schedule of dummy calculations to be inserted amidst calculations

4   using said secret exponent.

47.   The mobile terminal of claim 46 wherein said schedule of dummy

2   calculations comprises dummy multiplications associated with a small fraction of the bits of said

exponent which are equal to one particular binary bit polarity.

48.   The mobile terminal of claim 34 wherein said device comprises a smart

2   card.

49.   The mobile terminal of claim 34 wherein said device comprises a subscriber

2   identity module.

50.   The mobile terminal of claim 34 wherein said secret number comprises a

2   private cryptographic key.

ABSTRACT OF THE DISCLOSURE

A mobile terminal for use in a mobile communications system includes a SIM card storing subscriber related data. For security, the SIM card performs secret cryptographic calculations with secret numbers. Secret information is hidden from outside observation by scheduling the calculations using a precomputed, fixed randomization schedule in such a way

5   that externally observable parameters of the device cannot be associated to particular pieces, bits, symbols or values of the secret information.

FIG. 1

CRYPTOGRAPHIC
MULTIPLIER 26

12

CONNECTOR 30

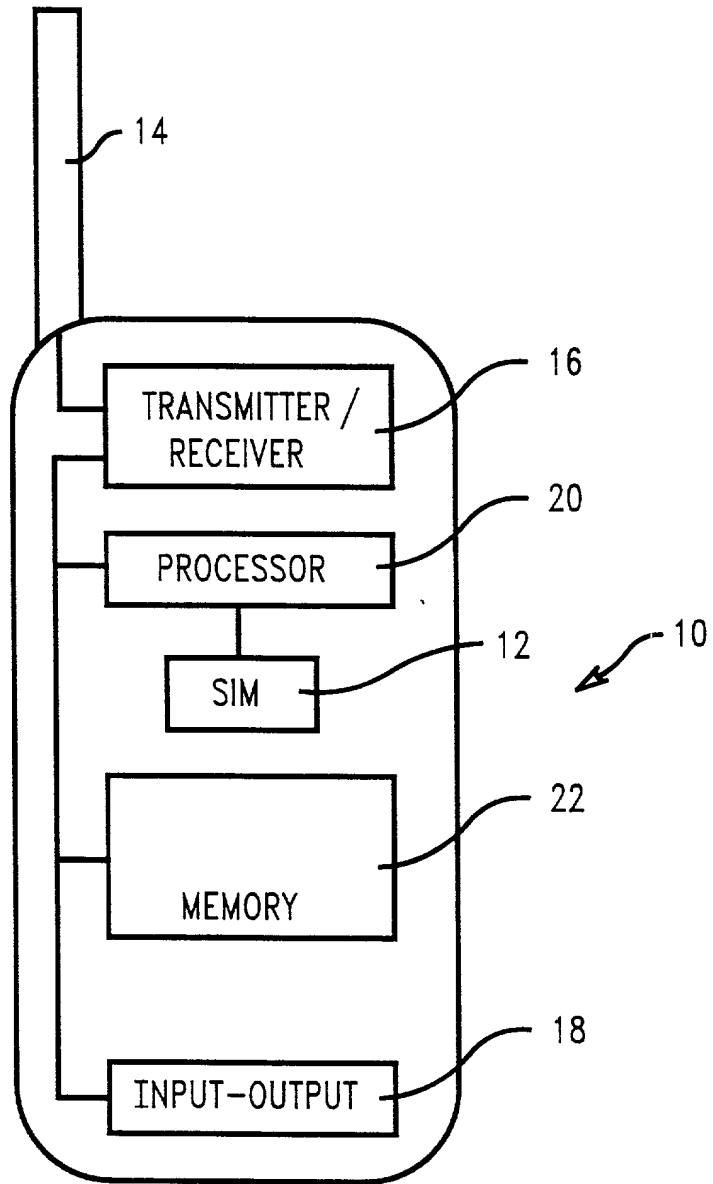PROCESSOR

24

SHUNT
REGULATOR 32

MEMORY 28

FIG. 2

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name; that

I verily believe I am the original, first and sole inventor (if only one name is listed below) or a joint inventor (if plural inventors are named below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: "Method for Masking Secret Multiplicands" ,
the specification of which:

☐ is attached hereto.   ☐ was filed on _____
                              as Application Serial No. _____
                              and was amended on _____
                                                          (if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment specifically referred to above, and that I believe the named inventor(s) to be the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought, and hereby acknowledge the duty to disclose information which is material to the patentability of the application in accordance with §1.56 (reprinted on the back) of Title 37 of the Code of Federal Regulations

I also hereby state that no patent applications on this invention have previously been filed in countries foreign to the United States of America, except as follows:

COUNTRY	APPLICATION NUMBER	DATE FILED (day, month, year)	PRIORITY CLAIMED UNDER 35 U.S.C. 119	
			yes	no
			yes	no
			yes	no

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

_____   _____   _____
(Application Serial No.)   (Filing Date)   (Status: patented, pending, abandoned)

_____   _____   _____
(Application Serial No.)   (Filing Date)   (Status: patented, pending, abandoned)

I hereby appoint Richard S. Phillips (Reg. No. 17,314), Wm. A. VanSanten (Reg. No. 22,810), Jeffrey L. Clark (Reg. No. 29,141), John S. Mortimer (Reg. No. 30,407), F. William McLaughlin (Reg. No. 32,273), and Dean A. Monco (Reg. No. 30,091), each registered to practice before the United States Patent and Trademark Office and practicing as the firm of **WOOD, PHILLIPS, VAN SANTEN, CLARK & MORTIMER, 500 WEST MADISON STREET, SUITE 3800, CHICAGO, ILLINOIS 60661 (Telephone 312-876-1800)**, and Charles L. Moore, Jr. (Reg. No. 33,742), David G. Matthews (Reg. No. 33,959), Kevin A. Sembrat (Reg. No. 36,673), Debra K. Stephens (Reg. No. 38,211), David K. Purks (Reg. No. 40,133), Mark C. Terrano (Reg. No. 40,200), Stephen A. Calogero (Reg. No. 41,491), Herbert V. Kerner (Reg. No. 42,721), Kermit D. Lopez (Reg. No. 41,953), and Kenneth W. Bolvin (Reg. No. 34,135), and my attorneys with full power of substitution and revocation, to prosecute this application, to make alterations or amendments therein, to receive the patent and to transact all business in the Patent and Trademark Office connected therewith, and direct that all correspondence be addressed to the firm. All telephone inquiries may be directed to:

_____ Dean A. Monco _____

§1.56 Duty to disclose information material to patentability.

(a)   A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclose information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any exists claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§ 1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

        (1)   prior art cited in search reports of a foreign patent office in a counterpart application, and

        (2)   the closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentability defines, to make sure that any material information contained therein is disclosed to the Office.

(b)   Under this section, information is material to patentability when it is not cumulative to information already of record or being made of record in the application, and

        (1)   It establishes, by itself or in combination with other information, a prima facie case of unpatentability of a claim; or

        (2)   It refutes, or is inconsistent with, a position the applicant takes in:

            (i)   Opposing an argument of unpatentability relied on by the Office, or

            (ii)   Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c)   Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

        (1)   Each inventor named in the application;
        (2)   Each attorney or agent who prepares or prosecutes the application; and
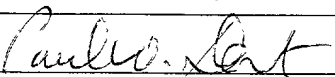   (3)   Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d)   Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent or inventor.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.
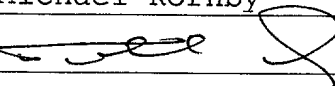
Full name of sole or
first Joint Inventor _Paul W. Dent_   Citizenship _GREAT BRITAIN_

Inventor's Signature _Paul W. Dent_   Date _6 Nov 2000_

Residence _637 Eagle Point Road, Pittsboro, North Carolina 27312_

Post Office Address _c/o Ericsson Inc., 7001 Development Drive, P. O. Box 13969, Research Triangle Park, North Carolina 27709_

Full name of second
Joint Inventor, if any _Michael Kornby_   Citizenship _SWEDEN_

Inventor's Signature _____   Date _6 Nov 2000_

Residence _125 Lochwood West Drive, Cary, North Carolina 27511_

Post Office Address _c/o Ericsson Inc., 7001 Development Drive, P. O. Box 13969, Research Triangle Park, North Carolina 27709_

Full name of third
Joint Inventor, if any _____   Citizenship _____

Inventor's Signature _____   Date _____

Residence _____

Post Office Address _____

Full name of fourth
Joint Inventor, if any _____   Citizenship _____

Inventor's Signature _____   Date _____

Residence _____

Post Office Address _____

Full name of fifth
Joint Inventor, if any _____   Citizenship _____

Inventor's Signature _____   Date _____

Residence _____

Post Office Address _____